UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,439	08/30/2000	Douglas B. Moran	RECOP011	2559

21912 7590 03/10/2004

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	8

DATE MAILED: 03/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/651,439	MORAN, DOUGLAS B.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 August 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 have been examined.

Priority

The following is a quotation of the appropriate part of 35 U.S.C. 120:

> An application for patent for an invention disclosed in the manner provided by the first paragraph of section 112 of this title in an application previously filed in the United States, or as provided by section 363 of this title, which is filed by an inventor or inventors named in the previously filed application shall have the same effect, as to such invention, as though filed on the date of the prior application, if filed before the patenting or abandonment of or termination of proceedings on the first application or on an application similarly entitled to the benefit of the filing date of the first application and if it contains or is amended to contain a specific reference to the earlier filed application.

2. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows: the application to which the instant application has been filed as a continuation, U.S. Patent Application No. 09/615,967, filed 14 July 2000, has no inventors in common with the instant application.

3. The instant application claims priority to Provisional U.S. Patent Application No. 60/151,531, filed 30 August 1999.

Information Disclosure Statement

4. The following Information Disclosure Statement in the instant application has been fully considered:

Paper No. 4, filed 16 April 2001.

5. Three additional documents have been found in the file wrapper that were not listed on the Form PTO-1449:

Lunt, et al., "Automated Audit Trail Analysis and Intrusion Detection: A Survey, " October, 1988.

Farmer et al., "The COPS Security Checker System," 1990.

Porras et al., "EMERALD : Event Monitoring Enabling Responses to Anomalous Live Disturbances," date unknown.

Each has been fully considered.

Drawings

6. The drawings are objected to under 37 CFR 1.74 and 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, reference numbers for the claimed features, as depicted in Figure 6, must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

7. The drawings are objected to as failing to comply with 37 CFR 1.84(l) because the lines in Figure 2 are not uniformly thick and well-defined. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 7-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 7 provides for the use of continuations, but, since the claim does not set forth any limitations defining the way in which they are to be used, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced. In view of the fact that the

specification notes that the use of continuations in computer software occurs in many instantiations (see page 87, lines 7-10), claim 7 will be considered to stand or fall with base claim 5.

Claims 8-12 depend from rejected claim 7, and include all the limitations of that claim, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 1-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The language of the claims raises a question as to whether the claims are directed merely to abstract ideas that are not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. See MPEP §2106 IV.B2(c).

10. Claims 7-12 are rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153

USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966). This is related to the rejection of claims 7-12 under 35 U.S.C. 112, above.

11. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (nonstatutory) and 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

12. Claims 1-17 are rejected under 35 U.S.C. 102(a) as being anticipated by U.S. Patent No. 5,694,590 to Thuraisingham et al.

As per claims 1 and 16, Thuraisingham uses a rules-based knowledge engine for analyzing collected data (see column 2, line 38 to column 3, line 16 and claim 2), and uses forward- and backward-chaining in analysis (see column 17, lines 15-43 and column 24, lines 17-42).

As per claim 2, the use of frame-based reasoning allows a limitation on the length of chaining (see column 17, line 59 to column 18, line 7).

As per claims 3 and 4, the backward-chaining, described above, has a goal defined in the ACTION part and sub-goals defined in the CONDITION part.

As per claims 5 and 7, the use of fuzzy reasoning with backward-chaining would entail scores being associated with goals (see column 18, line 20 to column 19, line 16).

As per claim 6, the invention uses reliability values, which are confidence factors (see column 20, lines 39-51).

As per claim 8, the use of fuzzy reasoning with forward-chaining would result in the use of scores for determining goals.

As per claim 9, the system is designed to detect computer security violations (see abstract).

As per claims 10 and 11, multiple levels of nets are disclosed, which are sources of facts (see column 4, line 66 to column 5, line 7 and column 7 lines 43-51), and are inputted in the Knowledge Acquisition process (see column 16, line 50 to column 17, line 15). Indirect facts are produced by the Truth Maintenance System (see column 21, lines 17-61).

As per claim 12, all phases of an attack can be analyzed.

As per claim 13, fuzzy reasoning is designed to address incomplete facts.

As per claims 14 and 15, there is a user interface capable of accepting and communicating all pertinent information (see abstract).

As per claim 17, computer implementations are disclosed (see columns 23 and 24).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Lee et al., "Mining in a data-flow environment: experience in network intrusion detection", 18 August 1999, discloses the use of data-mining methods in intrusion detection.

U.S. Patent No. 5,960,170 to Chen et al. discloses the use of inference rules for virus detection.

U.S. Patent No. 5,958,050 to Griffin et al. discloses the use of rules to determine trustworthiness.

U.S. Patent No. 6,519,703 to Joyce discloses the use of heuristic reasoning in firewalls.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

March 5, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100